# Oracle Access Governance

Oracle Access Governance is a cloud native identity governance and administration (IGA) service that provides customers with a simple, easy-to-understand view of what resources individuals can access, whether they should have that access, and how they're using their access entitlements.

Businesses are challenged every day to enforce appropriate, just-in-time user access rights to manage control of their information and address regulatory compliance requirements regarding least-privilege access. By providing immediate and prescriptive guidance about the types of access users should have, Oracle Access Governance makes it easier for administrators to provision new users and deprovision departing users quickly. In addition, machine learning intelligence in Oracle Access Governance can monitor all types of access to identify anomalous behavior patterns and automate remediation actions as required. Oracle Access Governance supports continuous compliance with proper access management and constantly evaluates and reports risks, allowing organizations to avoid big, manual, periodic reviews and significantly reducing the cost and effort of audit responses. Events and access at risk are reviewed regularly, and reviews are informed by built-in intelligence. Oracle Access Governance continuously adds support for orchestrated systems, providing strong insights into access controls across new applications that may span cloud and on-premises environments.

## Background

Traditionally, organizations of all sizes across industries have encountered challenges in effectively managing access levels for users, devices, bots, and services. These challenges include enhancing productivity while minimizing potential risks, maintaining visibility into who has access to which digital asset, and verifying the validity of such access in accordance with company compliance guidelines.

Organizations typically rely on manual processes to assign permissions to users and other identities. This often involves users reaching out to other individuals through email or collaboration tools to request access. However, manual processes pose challenges in terms of scalability and compliance verification. Many organizations also depend on periodic manual reviews of access rules, entitlements, permissions, roles, and policies.

The global increase in cloud adoption and digital transformation has compelled organizations to be aware of the security risks associated with access and entitlements. With the prevalence of multicloud and hybrid environments, organizations face the challenge of effectively managing the accurate and automated provisioning and deprovisioning of user access. Additionally, the complex and time-consuming nature of access reviews and the lack of necessary context make it difficult for reviewers to make informed decisions about an individual's access. This lack of clarity leads many organizations to take a "rubber-stamp approval" approach, providing blanket approvals that don't

Governance and compliance
Identity intelligence
Access control
Identity orchestration

Oracle Access Governance continuously discovers identities, monitors their privileges, learns usage patterns, automates access review and compliance processes, and offers prescriptive recommendations to support compliance and provide greater visibility into access across an organization's entire cloud and on-premises environment.

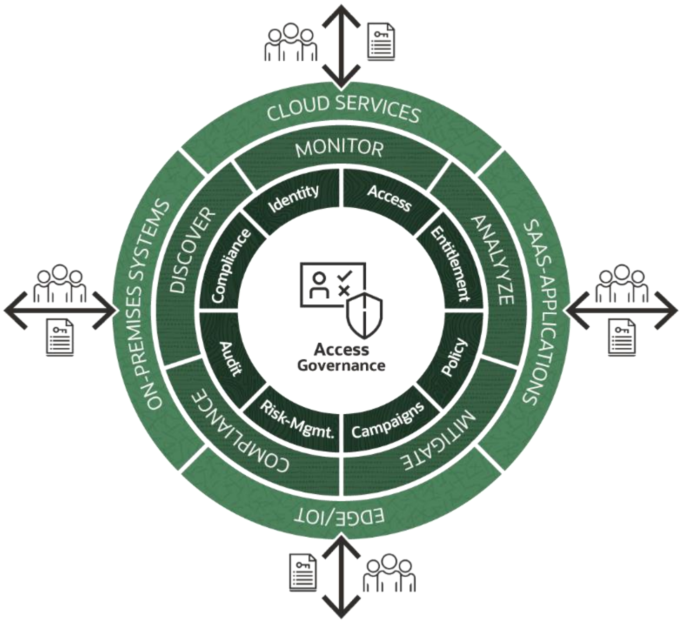
> "As we steer our path towards the adoption of a cloud native governance architecture, Oracle Access Governance rises as a critical player in this arena. Its strategic design, emphasizing intuitive user access review, prescriptive analytics powered by data insights, and automated remediation, echoes our commitment to fostering a secure IT environment. This cloud native service aligns perfectly with our forward-looking IT security strategy, and we are eager to explore its potential."

**Chinna Subramaniam**
Director, IAM and Directory Services, Department of Technology, City and County of San Francisco

revoke overprivileged access. These issues make it hard for organizations to minimize or eliminate the risks associated with identity access to digital assets and overprivileged access to critical data, prove compliance with corporate policies, and reduce governance costs.

## Overview

To leverage advanced identity governance and administration capabilities and improve productivity, organizations should evaluate solutions that offer flexible access control measures. These solutions should incorporate real-time capabilities, such as prescriptive analytics, that effectively identify anomalies and mitigate security risks. By evaluating and implementing such solutions, organizations can bolster their security posture and streamline identity governance processes.



Oracle Access Governance—governance that's always on

Oracle Access Governance is a comprehensive governance solution that supports various provisioning methods, including access requests and approvals, role-based access control (RBAC), attribute-based access control (ABAC), and policy-based access control (PBAC). The service features a conversation-style user experience, offering deep visibility into access permissions across the entire enterprise. It facilitates dynamic, periodic, and automated event-based micro certifications, such as an access review triggered by a job code or manager change. Additionally, it enables near real-time access reviews, providing detailed recommendations with options for reviewers to accept or review an entitlement based on the identified level of risk.

Oracle Access Governance can also run with Oracle Identity Governance in a hybrid deployment model. Organizations that opt for a hybrid model can take advantage of advanced capabilities available from cloud native services while retaining parts of their on-premises identity and access management suite to address compliance or data residency requirements.

"With our transition to a cloud-based governance solution, Oracle Access Governance presents an appealing option for streamlining user access reviews, providing enterprise-wide visibility into access permissions, ensuring zero migration effort, and offering insight-driven analytics. We believe it has the potential to enhance our IT security and efficiency, making it a worthwhile solution for organizations exploring cloud governance platforms."

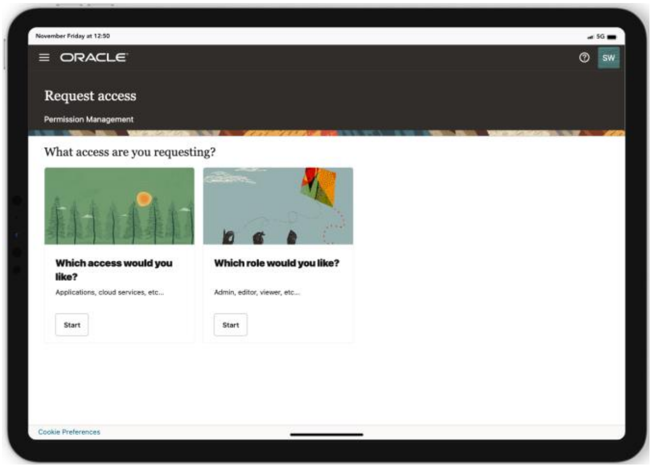
**Monica J. Field**
IT Director, Identity and Access Management, Cummins Inc.

"We see tremendous value when leveraging identity-as-a-service solutions, such as Oracle Access Governance, to integrate more powerful, analytics-driven security for organizations moving to the cloud. This solution enables Deloitte professionals to deliver enhanced security with agility, scale, and analytics, all while helping clients protect their existing investments in governance and supporting multi-cloud environments."

**Kashif Dhatwani**
Advisory Senior Manager, Cyber and Strategic Risk, Deloitte

## Key benefits

- **Simplified self-service:** Oracle Access Governance provides self-service capabilities that empower end users to request access bundles or roles for themselves or others while enabling the help desk to manage account lifecycles. This streamlined process enhances efficiency and empowers users to actively participate in access governance activities.


November Friday at 12:50
ORACLE
SW
Request access
Permission Management
What access are you requesting?
Which access would you like?
Applications, cloud services, etc...
Start
Which role would you like?
Admin, editor, viewer, etc...
Start
Cookie Preferences

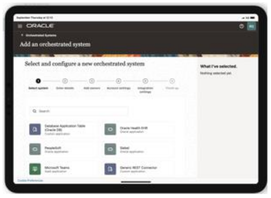
Simplified self-service

- **Simplified identity orchestration:** Oracle Access Governance offers low-code integration capabilities, allowing application owners to quickly and efficiently onboard applications and services into Access Governance. This streamlines identity orchestration processes, reducing both time and cost.
- **Automated access control:** Oracle Access Governance supports identity collections, which enables attribute-based access control. This capability allows for fine-grain control over access bundles based on specific attributes associated with identities. Furthermore, Oracle Access Governance incorporates role-based access control, a feature that enables access rights to be defined and managed based on specific roles. These identity collections and roles can be further used by policy-based access control to grant and manage access rights. Unmatched account certifications help detect orphaned and rogue accounts in various governed systems.
- **Access guardrails:** Oracle Access Governance allows users to define constraints on access bundles, facilitating compliance with prerequisites such as attribute verification and permission checks. These constraints can be applied in various scenarios—examples include requiring training completion before granting privileged access, verifying citizenship before allowing access to sensitive systems, and enabling only administrators to request access to confidential reports. These access guardrails safeguard application owners by establishing certain segregation of duties (SoD) rules. Oracle Access Governance also raises potential conflicts as part of the access

### Key features

Oracle Access Governance includes a robust set of features, including the following:

- **Cloud native service**: It's an OCI native subscription service.
- **Intuitive user experience**: It offers an intuitive user experience using a conversational approach.
- **Interactive dashboards**: Its dashboards offer valuable insights that help users focus on essential tasks.
- **Enterprise-wide browser**: Its analytics-driven dashboard gives privileged users deep visibility into all access information.
- **Identity orchestration:** It supports rapid application onboarding with a low-code, wizard-based integration approach that includes correlation and transformation rules.
- **Easy integrations:** It offers a wide range of specialized and generic integrations through downloadable container-based agents, RESTful APIs, and flat files.

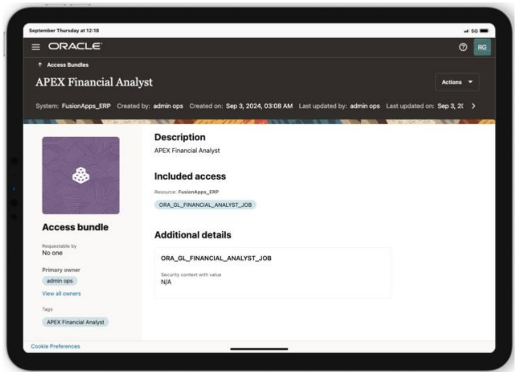


Application catalog

- **Wide range of integrations:** It offers identity orchestration for various Oracle workloads, such as OCI, Oracle Cloud Applications, Oracle EHR, and Oracle Database, and non-Oracle workloads, such as Microsoft AD, Entra ID, MS SQL, IBM DB2, SAP Ariba, S4 HANA, and ARCON PAM.
- **Simplified access request:** It provides a simple user

request approval task using SoD rules defined in Oracle Fusion Cloud Risk Management and Compliance.

- **Flexible delegated access control:** Oracle Access Governance facilitates delegated ownership, which allows businesses to manage identity collections while application owners oversee access bundles, including accounts and entitlements. This delegation supports the efficient and streamlined management of access rights within Oracle Access Governance and promotes collaboration and accountability among stakeholders.



APEX Financial Analyst

System: FusionApps_ERP Created by: admin ops Created on: Sep 3, 2024, 03:08 AM Last updated by: admin ops Last updated on: Sep 3, 2(

Description
APEX Financial Analyst

Included access
Resource: FusionApps_ERP
ORA_GL_FINANCIAL_ANALYST_JOB

Additional details
ORA_GL_FINANCIAL_ANALYST_JOB
Security context with value
N/A

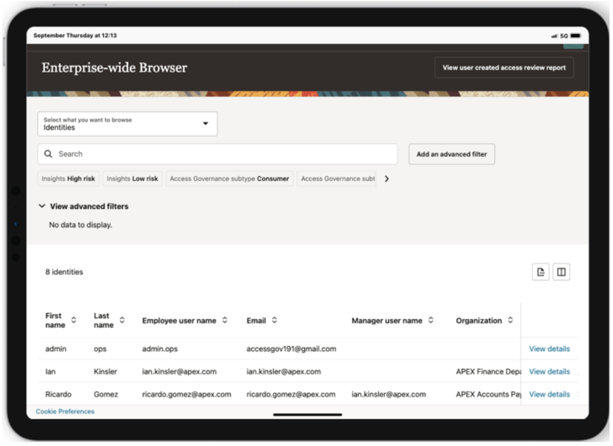
Requestable by
No one

Primary owner
admin ops

Tags
APEX Financial Analyst

Configuring an access bundle with various permissions

- **Visibility into enterprise-wide access:** Oracle Access Governance offers visibility into user access across the entire organization, providing insights into which users have access to specific applications, resources, and services. Managers can review their team's access map, enabling them to understand and oversee the access privileges of their team members. Individual users can also view their own access permissions, giving them transparency into and awareness of their own access rights.



Select what you want to browse
Identities

Insights High risk | Insights Low risk | Access Governance subtype Consumer | Access Governance subt

No data to display.

8 identities

| First name | Last name | Employee user name | Email | Manager user name | Organization | |
|---|---|---|---|---|---|---|
| admin | ops | admin.ops | accessgov191@gmail.com | | | View details |
| Ian | Kinsler | ian.kinsler@apex.com | ian.kinsler@apex.com | | APEX Finance Depa | View details |
| Ricardo | Gomez | ricardo.gomez@apex.com | ricardo.gomez@apex.com | ian.kinsler@apex.com | APEX Accounts Pay | View details |

Visibility into enterprise-wide access

- **Improve certification efficiency**: Oracle Access Governance empowers organizations with actionable insights and prescriptive analytics, facilitating a comprehensive understanding of the necessary access required to expedite user productivity. Event-based certifications, triggered, for example, by a job or organization change, and timeline-based certifications allow access reviewers to quickly take the necessary actions to update access experience for self-service-based requests.

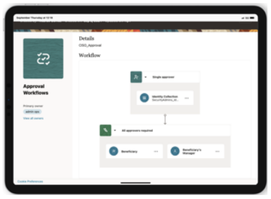
- **Automated access control:** It provides multiple access control measures and guardrails that can be used to automate access in various scenarios.

- **Access bundle mining:** It automates the creation of access bundles based on permissions and their assignments within the orchestrated system.

- **Actionable access reviews:** It simplifies the access review process and provides actionable insights based on prescriptive analytics so managers can make informed decisions.

- **Micro certifications:** It facilitates intelligent event-based access reviews, triggered only when there are changes in the system of record. Timeline-based micro certifications help in the timely review of accesses based on important milestones. Unmatched account certifications get triggered when orphaned and rogue accounts are detected.

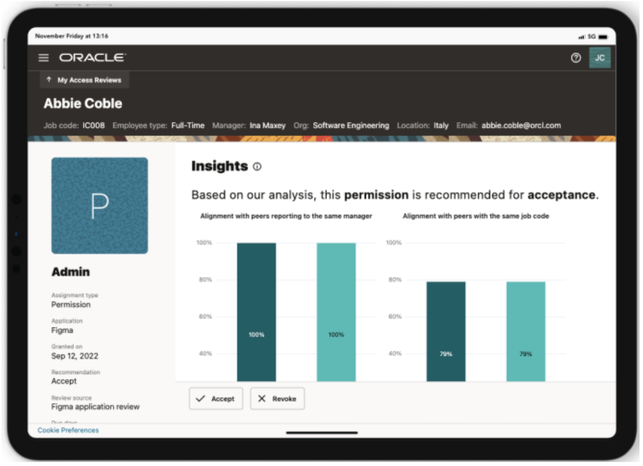
- **Codeless workflows:** It provides lightweight, codeless workflows for access control and governance.



Workflow editor

- **Configurable notifications:** It includes customizable notifications that can be delivered either by a native or OCI notification delivery service.

- **Comprehensive IT audits and reporting:** It includes simplified auditing, privileges. Policy and group reviews help further enforce the principle of least privilege.


November Friday at 13:16

ORACLE

My Access Reviews

Abbie Coble

Job code: IC008 Employee type: Full-Time Manager: Ina Maxey Org: Software Engineering Location: Italy Email: abbie.coble@orcl.com

Admin

Assignment type
Permission

Application
Figma

Granted on
Sep 12, 2022

Recommendation
Accept

Review source
Figma application review

Insights

Based on our analysis, this **permission** is recommended for **acceptance**.

5G
JC
P
Alignment with peers reporting to the same manager
Alignment with peers with the same job code
100%
80%
60%
40%
100%
100%
100%
80%
60%
40%
79%
79%
Accept
Revoke
Cookie Preferences

Enforce access controls with prescriptive analytics

- **Governance anywhere:** Oracle Access Governance provides governance across enterprise applications and IaaS, PaaS, and SaaS workloads, including Oracle and non-Oracle workloads. Oracle Access Governance is purpose-built for Oracle workloads to enable simplified governance and facilitate real-time security, compliance, and operational efficiency. The same capabilities are extended to several non-Oracle workloads as well.
- **Extended analytics:** Oracle Access Governance collects data from multiple orchestrated systems and publishes the identity and access updates as events in real time to Oracle Cloud Infrastructure (OCI) Events Service. This enables the seamless flow of data from orchestrated sources to business intelligence tools and analytics services, which may be consuming data from other sources too, allowing for enhanced analysis.
- **Enhanced regulatory compliance:** Oracle Access Governance helps enforce and attest to regulatory requirements—such as Sarbanes-Oxley, 21 CFR Part 11, Gramm-Leach-Bliley, HIPAA, and GDPR—that are associated with identifying who has access privileges to sensitive, high-risk data.
- **Reduced costs:** Oracle Access Governance allows organizations to use a cloud native identity governance service that helps reduce IT costs and save time through efficient, user-friendly dashboards, codeless workflows, and wizard-based application onboarding.

monitoring, and flexible reporting capabilities.

ORACLE

ad2016system

There are **4,000 identities** that can access this resource.

Analytics dashboard

## Summary

Oracle Access Governance helps organizations automate access control, gain visibility into enterprise-wide access, make informed access decisions, and support their overall compliance objectives. Organizations can extend their current identity governance and administration capabilities with a cloud native service to gain deeper insights. For more information, review the Oracle Access Governance product documentation or visit the Oracle Access Governance webpage.

### Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle